A refined formula of the relative class number of an imaginary abelian field

Hiroshi YAMASHITA

Abstract. Let p be an odd prime. Let F be an imaginary abelian field where the prime p is unramified. Let e be an idempotent element contained in the group ring of the Galois group with coefficients in the ring of p-adic integers. Let A be the p-primary part of the relative class group of F. We prove a formula describing the order of eA. This formula is considered as a refinement of the relative class number formula.

Introduction. We assume p is an odd prime number. The class numner of the relative class group of an imaginary abelian field is described as a product of generalized Bernoulli numbers relative to odd Diriclet characters χ corresponding to the field and auxiliary factors Q (the unit index), W (the number of roots of unity contained in the field) *c.f.* [9, Theorem 4.17]:

$$QW\prod_{\chi} -\tfrac{1}{2}B_{1,\chi^{-1}}.$$

This value is a positive integer. So, we can study the p-primary part of this integer. The purpose of this note is to show a refinment of this formula when we restrict our concern to its p-part. We note that $-B_{1,\chi^{-1}}$ is equal to the value of the Diriclet L-function $L(s,\chi^{-1})$ at $s=0$. We use $L(0,\chi^{-1})$ in place of $-B_{1,\chi^{-1}}$. Now, we state the precise definition of the relative class group. Let F be an imaginary abelian extension of finite degree over $\mathbf{Q}$. Its relative class group is defined to be a subgroup of the ideal class group C_F consisting of ideal classes whose norm into the class group of the maximal real subfield is the unit class.

Let $\mathbf{Z}_p$ be the ring of p-adic integers. To study the p-Sylow subgroup of the relative class group, we extend coefficients onto $\mathbf{Z}_p$. We have the extension $\mathbf{Z}_p \otimes C_F$ is isomorphic to the p-Sylow subgroup of C_F and its order is equal to the p-part of the value of the above product. Moreover, since the Galois group G of $F/\mathbf{Q}$ acts on C_F, we can consider $\mathbf{Z}_p \otimes C_F$ is a module over the group ring with coefficients in $\mathbf{Z}_p$. This group ring is denoted by $\mathbf{Z}_pG$. Accordingly, we can apply the theory of representation of $\mathbf{Z}_pG$ and interpret the characters appearing in the above relative class number formula as characters affforded by some representation modules.

Let ρ be the map of complex conjugation. $e^- = (1-\rho)/2$ is an idempotent element contained in the group ring and $e^-\mathbf{Z}_p \otimes C_F$ is isomorphic to the p-Sylow subgroup of the relative class group. Denote by $\mathbf{Q}_p$ the field of fractions of $\mathbf{Z}_p$. Let $\bar{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$, and let v_p be the valuation of $\bar{\mathbf{Q}}_p$ satisfying $v_p(p) = 1$. We fix an embedding of

平成 20 年 10 月 1 日受理

algebraic closure of $\mathbf{Q}$ into $\bar{\mathbf{Q}}_p$ once for all. As a consequence, we regard every character χ appearing in the relative class number formula as a character of G taking values in the field $\bar{\mathbf{Q}}_p$. There is a one dimensional $\bar{\mathbf{Q}}_p$-representation ρ_χ of G affording each character χ. Let e be an idempotent element contained in $e^-\mathbf{Z}_pG$. Denote by Φ_χ the set of characters satisfying $\rho_\chi(e) \neq 0$. We will abbreviate $\rho_\chi(e)$ to $\chi(e)$ in the below.

We observe that the index of the maximal power of p dividing the order of $e^-\mathbf{Z}_p \otimes C_F$ equals the simple sum of valuations of $L(0,\chi^{-1})$'s when the field F does not contain any primitive pth root of unity:

$$v_p(\sharp e^-\mathbf{Z}_p \otimes C_F) = \sum_{\chi(e^-)\neq 0} v_p(L(0,\chi^{-1})).$$

We will replace the idempotent e^- by an arbitrary idempotent element e contained in $e^-\mathbf{Z}_pG$. It is expected an alternative formula

$$(1) \quad v_p(\sharp e\mathbf{Z}_p \otimes C_F) = \sum_{\chi(e)\neq 0} v_p\left(L(0,\chi^{-1})\right)$$

holds. This formula means that each direct factor of the finite $\mathbf{Z}_pG$-module $e^-\mathbf{Z}_p \otimes C_F$ corresponds the values at 0 of Diriclet L-functions, correctly. We shall give a proof of this formula. We note this formula (1) follows from [7, §10, Theorem 2] if the exponent of the abelian group G divides $p-1$.

As preparation, we give a brief investigation on the idempotent element of the group ring $\mathbf{Z}_pG$, here. Let G_p be the p-Sylow subgroup of G. There is a p'-subgroup G_0 such that $G = G_0 \times G_p$. This decomposition leads to the tensor decomposition of the ring $\mathbf{Z}_pG$: $\mathbf{Z}_pG_0 \otimes_{\mathbf{Z}_p} \mathbf{Z}_pG_p$. The ring $\mathbf{Z}_pG_0$ is a semiperfect ring *c.f.* [1,§6C]. More concretely, since $\mathbf{Z}_p$ is a valuation ring, the ring $\mathbf{Z}_pG_0$ is a direct sum of valuation rings over $\mathbf{Z}_p$. On the contrary, the ring $\mathbf{Z}_pG_p$ is a local ring. Therefore, by the theorem of lifting idempotens, *c.f.* [1, §6A, Theorem 6.7], each idempotent element of $\mathbf{Z}_pG$ comes from those of $\mathbf{Z}_pG_0$. Namely, it is obtained as a tensor product of an idempotent of $\mathbf{Z}_pG_0$ and the identity element of $\mathbf{Z}_pG_p$: $e_0 \otimes 1$. Furthermore, we also decompose each character χ of G into a product of a character of χ_0 of G_0 and χ_p of G_p : $\chi = \chi_0\chi_p$. Let Φ_e be the set of characters χ satisfying $\chi_0(e_0) \neq 0$, where $e = e_0 \otimes 1$. Suppose e_0 is a primitive idempotent element. If we take a character χ from the set Φ_e, then the factor χ_0 concerning G_0 and the factor for every $\chi' \in \Phi_e$ is conjugate to each other. Namely, there is a $\mathbf{Q}_p$-automorphism σ of $\bar{\mathbf{Q}}_p$ for χ and χ' contained in Φ_e such that $\chi'_0 = \sigma \circ \chi_0$. Φ_e is a set of characters $\chi_0\chi_p$ such that χ_0 is contained in a conjugate class of characters of G_0.

1 $\mathcal{O}G$-lattices. Let $\mathbf{C}_p$ be the completion of $\bar{\mathbf{Q}}_p$ with the metric induced by the valuation. We denote by the same symbol v_p an extension of the valuation v_p on $\mathbf{C}_p$. Let $\mathcal{K}$ be a finite extension of $\mathbf{Q}_p$ contained in C_p. Let $\mathcal{O}$ be the valuation ring. We define a rational number $\ell_{\mathcal{O}}(M)$ for an $\mathcal{O}$-module M of finite order to be $\ell_{\mathcal{O}}(M) = m/e$ if the length of $\mathcal{O}$-composition series is equal to m and if the ramification index of $\mathcal{K}$ is e. This value of the length is constant for extension of coefficients. More precisely, if $\mathcal{K}'$ is a finite extension of $\mathcal{K}$ whose ramification index over $\mathbf{Q}_p$ is e'

and whose valuation ring is $\mathcal{O}'$ and if the length of $\mathcal{O}'$-composition series of $\mathcal{O}' \otimes_{\mathcal{O}} M$ is m', we have $m'/e' = m/e$. If no confusion may occurs, we denote by $\mathcal{O}'M$ except for $\mathcal{O}' \otimes_{\mathcal{O}} M$ and denote by $\ell(M)$ the value of $\ell_{\mathcal{O}}(M) = \ell_{\mathcal{O}'}(\mathcal{O}'M)$, hereafter. We note $\ell(\mathcal{O}/\alpha\mathcal{O}) = v_p(\alpha)$ holds for an arbitrary element $\alpha \neq 0$ of $\mathcal{O}$.

We call a free $\mathcal{O}$-module of finite rank an $\mathcal{O}$-lattice. Let G be a finite abelian group. Let $\mathcal{O}G$ be the group ring of G with coefficients in $\mathcal{O}$. If an $\mathcal{O}G$-module is simultaneously an $\mathcal{O}$-lattice, we call it an $\mathcal{O}G$-lattice. We suppose that every characters of G have their values in the valuation ring $\mathcal{O}$. Let

$$e_\chi = \frac{1}{\sharp G} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}.$$

be the idempotent element associated with a character χ in the group ring $\mathcal{K}G$. If $v_p(\sharp G) \neq 0$, this idempotent does not belong to the integral group ring $\mathcal{O}G$. Let M be a $\mathbf{Z}_pG$-lattice. We abbreviate $\mathcal{O} \otimes_{\mathbf{Z}_p} M$ to $\mathcal{O}M$. Since M is $\mathbf{Z}_p$-free, we consider this module as a submodule of the $\mathcal{K}$-vector space $\mathcal{K}M$. The χ-part M^χ is a submodule of $\mathcal{O}M$ defined to be

$$M^\chi = \{x \in \mathcal{O}M : \forall\sigma \in G, \sigma x = \chi(\sigma)x\}.$$

However, if we say *χ-part of M* in this paper, it means a submodule of $\mathcal{K}M$ denoted by M_χ and defined to be

$$M_\chi = \{e_\chi x : x \in \mathcal{O}M\}.$$

Clearly, we see $M^\chi \subset M_\chi$ and $(\sharp G)M_\chi \subset M^\chi$. Hence, M^χ is a sublattice of M_χ of finite index. Denote by pr_M restriction onto $\mathcal{O}M$ of the projection map of $\mathcal{K}M$ onto the eigen space $e_\chi\mathcal{K}M$. The χ-part M_χ is the image of pr_M, and hence $M_\chi \cong \mathcal{O}M/\mathrm{Ker}\, pr_M$. If a quotient module N of the $\mathbf{Z}_pG$-lattice M by a $\mathbf{Z}_pG$-sublattice L is also a $\mathbf{Z}_pG$-lattice, there is a $\mathcal{K}G$-homomorphism $\varphi : \mathcal{K}M \to \mathcal{K}N$ such that $\mathrm{Ker}\,\varphi \cong \mathcal{K}L$. Hence, we have a sequence

$$L_\chi \xrightarrow{\iota} M_\chi \xrightarrow{\varphi} N_\chi,$$

where the map ι is injective and $\varphi(M_\chi) = N_\chi$. However, this sequence is not always exact. There is an exact sequence composed of kernels of the projection maps:

$$0 \to \mathrm{Ker}\, pr_L \to \mathrm{Ker}\, pr_M \to \mathrm{Ker}\, pr_N.$$

Denote by $(\mathrm{Ker}\, pr_N)^*$ the image of $\mathrm{Ker}\, pr_M$ by φ. We have an exact sequence

$$0 \to L_\chi \to M_\chi \to \mathcal{O}N/(\mathrm{Ker}\, pr_N)^* \to 0.$$

We define N_χ^* to be M_χ/L_χ, which is isomorphic to $\mathcal{O}N/(\mathrm{Ker}\, pr_N)^*$. Since $(\mathrm{Ker}\, pr_N)^* \subset \mathrm{Ker}\, pr_N$, there is a canonical homomorphism of N_χ^* onto N_χ. Moreover, since N_χ is $\mathcal{O}$-free, this surjection splits. Thus, if $T_\chi(M;N)$ denotes a finite module $\mathrm{Ker}\, pr_N/(\mathrm{Ker}\, pr_N)^*$, we have $N_\chi^* \cong T_\chi(M;N) \oplus N_\chi$. If the quotient module $N = M/L$ is not a lattice, we define N_χ^* to be the quotient M_χ/L_χ. We treat this case only where N is of finite order.

We denote by $\hat{G}$ the set of characters of G. Since $\mathcal{K}M$ is a direct sum of eigen spaces $e_\chi\mathcal{K}M$, an $\mathcal{O}G$-sublattice $\tilde{M}$ generated by M_χ for every characters is an inner direct sum $\oplus M_\chi$. Since $1 = \sum_\chi e_\chi$ holds in $\mathcal{K}G$, the lattice $\mathcal{O}M$ is a sublattice of $\tilde{M}$ of finite index. For $N = M/L$, we denote by $\tilde{N}^*$ the dirct sum of N_χ^*:

$$\tilde{N}^* = \bigoplus_{\chi \in \hat{G}} N_\chi^*. \tag{2}$$

Let α (*resp.* β) be the inclusion map of $\mathcal{O}L$ (*resp.* $\mathcal{O}M$) into $\tilde{L}$ (*resp.* $\tilde{M}$) of an $\mathcal{O}G$-lattice. The inclusion map β induces an $\mathcal{O}G$-homomorphism of $\mathcal{O}N$ into $\tilde{N}^*$. Hence, we have the following commutative diagram consisting of two short exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{O}L & \to & \mathcal{O}M & \to & \mathcal{O}N & \to & 0 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 0 & \to & \tilde{L} & \to & \tilde{M} & \to & \tilde{N}^* & \to & 0. \end{array}$$

We apply the snake lemma to this diagram and obtain an exact sequence

$$0 \to \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha \to \operatorname{Coker}\beta \to \operatorname{Coker}\gamma \to 0.$$

Suppose N is of finite order. Since γ is a homomorphism between finite modules, the difference $\ell(\tilde{N}^*) - \ell(\mathcal{O}N)$ is equal to $\ell(\operatorname{Coker}\gamma) - \ell(\operatorname{Ker}\gamma)$. By the exact sequence, we obtain $\ell(\tilde{N}^*) - \ell(N) = \ell(\operatorname{Coker}\beta) - \ell(\operatorname{Coker}\alpha)$. The two terms $\operatorname{Coker}\beta = \ell(\tilde{M}/\mathcal{O}M)$ and $\operatorname{Coker}\alpha = \ell(\tilde{L}/\mathcal{O}L)$ in this equality can be determined from lattices M and L, independently. Furthermore, we can define similar quantity if an arbitrary pair of $\mathcal{O}G$-lattices is given, even if L is not a sublattice. Thus, denote by $\Delta(X;Y)$

$$\Delta(X;Y) = \ell(\tilde{X}/\mathcal{O}\otimes X) - \ell(\tilde{Y}/\mathcal{O}\otimes Y)$$

for two $\mathbf{Z}_pG$-lattices X and Y. We obtain the following formula

$$\ell(N) = \sum_{\chi\in\hat{G}} \ell(N_\chi^*) - \Delta(M;L), \tag{3}$$

taking account of (2), where $\ell(N_\chi^*)$ is the abridgement of $\ell_{\mathcal{O}}(N_\chi^*)$.

To prove the formula (1), we need to apply the Iwasawa theory in the successive sections. For this aim, we prepare a well-known lemma concerning Λ-modules. Let Λ be a ring of formal power series with indeterminate T and with coefficients in $\mathcal{O}$: $\Lambda = \mathcal{O}[[T]]$. Suppose that M is an $\mathcal{O}G$-lattice and a Λ-module simultaneously and that the action of $\mathcal{O}G$ on M commutes with the action of Λ. By the structure theorem of a finitely generated Λ-module, there exists a set $\{f_i\}_{1\leq i\leq r}$ of distinguished polynomials contained in Λ and an injective Λ-homomorphism $M \to \Lambda/f_1 \times \Lambda/f_2 \times \cdots \times \Lambda/f_r$ with finite cokernel. The product of these polynomials is uniquely determined for M and is called the characteristic polynomial of M.

Lemma 1. *Let f_M be the characteristic polynomial of M. If $T \nmid f_M$, we have $\ell(M/TM)$ equals the value of $v_p(f_M(0))$. Moreover, it is also equal to the sum of $\ell(M_\chi/TM_\chi)$.*

Proof. Denote by E the Λ-module $\Lambda/f_1 \times \Lambda/f_2 \times \cdots \times \Lambda/f_r$. We see $\ell(E/TE) = \sum_{i=1}^r v_p(f_i(0))$. The sum of the valuation of $f_i(0)$ coincides with $v_p(f_M(0))$. Therefore, we shall prove $\ell(M/TM) = \ell(E/TE)$. To this end, we may assume M is a submodule of E. Since $T \nmid f_M$, the multiplication of T on E is an injective endomorphism. Thus, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{T} & M & \to & M/TM & \to & 0 \\ & & \downarrow & & \downarrow & & \varphi\downarrow & & \\ 0 & \to & E & \xrightarrow{T} & E & \to & E/TE & \to & 0, \end{array}$$

where φ is a homomorphism induced from the inclusion $M \to E$. By the snake lemma, we have an exact sequence

$$0 \to \operatorname{Ker}\varphi \to E/M \to E/M \to \operatorname{Coker}\varphi \to 0.$$

Hence, $\ell(\operatorname{Ker}\varphi) = \ell(\operatorname{Coker}\varphi)$ holds. This implies $\ell(M/TM) = \ell(E/TE)$. Now, we apply the formula (3) to the pair of lattices M and TM, we obtain $\ell(M/TM)$ equals the value of $\sum_{\chi\in\hat{G}} \ell(M_\chi/TM_\chi) - \Delta(M;TM)$. Since $T \nmid f_M$, we see $M \cong TM$. It follows $\Delta(M;TM) = 0$. *q.e.d.*

2. **Z_p-lattices $\mathcal{U}$ and U.** We use the p-adic map defined in [2]. Let F be an imaginary abelian extension where p is unramified. Let G be the Galois group. Let Z be the decomposition field of p. Denote by $\mathfrak{g}$ the Galois group of Z. Let S (*resp.* S_F) be the set of prime ideals of Z (*resp.* F) dividing p. These sets of primes are $\mathfrak{g}$-set. Let $\iota_\mathfrak{p}$ be the embedding of Z into $\mathbf{C}_p$ corresponding to $\mathfrak{p} \in S$. Let $\mathcal{S}$ be the set of every embedding for $\mathfrak{p} \in S$. If we choose an ideal $\mathfrak{p}$ from S and fix it, we see $S = \{\sigma\mathfrak{p} : \sigma \in \mathfrak{g}\}$. Let U be a free $\mathbf{Z}_p$-module on the set S: $U = \oplus_{\mathfrak{p}\in S}\mathbf{Z}_p\mathfrak{p}$. Similarly, we denote by U_F a free $\mathbf{Z}_p$-module on the set S_F. We identify U_F with the image into U by the norm map $N_{F/Z}$. Put $n_{F/Z} = [F : Z]$. We see $U_F = n_{F/Z}U$. We define a homomorphism φ of $Z^\times$ into U by setting $\varphi(x) = \sum_{\mathfrak{p}\in S} v_p(\iota_\mathfrak{p}(x))\mathfrak{p}$. For F, we define φ_F to be $\varphi \circ N_{F/Z}$. These maps are extended onto $\mathbf{Z}_p \otimes Z^\times$ and $\mathbf{Z}_p \otimes F^\times$, respectively. We denote by the same symbol φ and φ_F these natural extension maps. Let $E_{1,Z}$ (resp. $E_{1,F}$) be the group of p-units of Z (*resp.* F). Denote by W (*resp.* W_F) the image of $\mathbf{Z}_p \otimes E_{1,Z}$ (*resp.* $\mathbf{Z}_p \otimes E_{1,F}$) by φ_Z (*resp.* φ_F). By class field theory,

$$Gal(\tilde{L}_F/L_F) \cong U_F/W_F, \tag{4}$$

where $\tilde{L}_F$ (*resp.* L_F) denotes the maximal unramified (*resp.* unramified and p-decomposed) abelian p-extension over F.

To avoid confusion, we introduce another $\mathbf{Z}_p\mathfrak{g}$-lattice $\mathcal{U}$ defined to be a free $\mathbf{Z}_p$-module on the set $\mathcal{S}$ where each $\sigma \in \mathfrak{g}$ acts by $\sigma\iota_\mathfrak{p} = \iota_{\sigma\mathfrak{p}} = \iota_\mathfrak{p} \circ \sigma^{-1}$ for $\mathfrak{p} \in S$. Note $U \cong \mathcal{U} \cong \mathbf{Z}_p\mathfrak{g}$. Let $Z_\mathfrak{p}$ be the completion of $\iota_\mathfrak{p}(Z)$ in $\mathbf{C}_p$. This field is called the completion of Z at $\mathfrak{p}$ in short. Let $Z_{\mathfrak{p},\infty}$ be the cyclotomic $\mathbf{Z}_p$-extension of $Z_\mathfrak{p}$. There is a reciprocity map $Z_\mathfrak{p}^\times/NZ_{\mathfrak{p},\infty}^\times \cong Gal(Z_{\mathfrak{p},\infty}/Z_\mathfrak{p})$ by local class field theory, where $NZ_{\mathfrak{p},\infty}^\times$ denotes the universal norm of $Z_{\mathfrak{p},\infty}^\times$ into $Z_\mathfrak{p}^\times$, that is, the intersection of images of norm maps of the multiplicative group of the nth layer of the $\mathbf{Z}_p$-extension into $Z_\mathfrak{p}^\times$ when n runs throughout the set of non-negative integers. The direct products $\prod_{\mathfrak{p}\in S} Z_\mathfrak{p}^\times$ and $\prod_{\mathfrak{p}\in S} NZ_{\mathfrak{p},\infty}^\times$ are considered as closed subgroups of the idèle group of Z. Since $Gal(Z_{\mathfrak{p},\infty}/Z_\mathfrak{p}) \cong \mathbf{Z}_p$, the quotient group $J_{Z,p} = \prod_{\mathfrak{p}\in S} Z_\mathfrak{p}^\times/NZ_{\mathfrak{p},\infty}$ is isomorphic to $\mathbf{Z}_p\mathfrak{g}$ as a $\mathbf{Z}_p\mathfrak{g}$-lattice. Here, we observe $Z_\mathfrak{p} = \mathbf{Q}_p$ and the universal norm $NZ_{\mathfrak{p},\infty}^\times$ is the closed subgroup of $\mathbf{Q}_p^\times$ generated by p and $(p-1)$th roots of unity. We notice the p-adic logarithm maps $Z_\mathfrak{p}^\times/NZ_{\mathfrak{p},\infty}^\times$ onto $\mathbf{Z}_p$ isomorphically and continuously. Hence, for an element $\mathfrak{x} = (x_\mathfrak{p}) \in J_{Z,p}$, we define an isomorphism onto the $\mathbf{Z}_p\mathfrak{g}$-lattice $\mathcal{U}$ by $\psi'(\mathfrak{x}) = \sum_{\mathfrak{p}\in S}(\frac{1}{p}\log_p x_\mathfrak{p})\iota_\mathfrak{p}$, where $\log_p$ denotes the p-adic logarithm. This map is an isomorphism between $\mathbf{Z}_p\mathfrak{g}$-lattices. Let $(\iota_\mathfrak{p}(x)) \in J_{Z,p}$ be the diagonal image of $x \in Z^\times$ into $J_{Z,p}$. Combining this diagonal map and ψ', we obtain a homomorphism of $Z^\times$ into $\mathcal{U}$. Similarly as in case of φ, it is extended onto $\mathbf{Z}_p \otimes Z^\times$, naturally. We denote by ψ this $\mathbf{Z}_p\mathfrak{g}$-homomorphism: $\psi(x) = \psi'((\iota_\mathfrak{p}(x)))$. We also define homomorphisms ψ'_F and ψ_F of $\mathbf{Z}_p\mathfrak{g}$-lattices for F. Precisely, we define the cyclotomic $\mathbf{Z}_p$-extension $F_{\mathfrak{p}',\infty}$ to be the compositum of $F_{\mathfrak{p}'}$ and $Z_{\mathfrak{p},\infty}$. Let $NF^{\times}_{\mathfrak{p}',\infty}$ be the universal norm of $F^{\times}_{\mathfrak{p}',\infty}$ into $F^{\times}_{\mathfrak{p}'}$. Put $J_{F,p} = \prod_{\mathfrak{p}' \in S_F} F^{\times}_{\mathfrak{p}'}/NF^{\times}_{\mathfrak{p}',\infty}$. Since every $\mathfrak{p} \in S$ inerts in F, the norm map $N_{F/Z}$ induces an isomorphism $J_{F,p} \cong J_{Z,p}$. Thus, we define $\psi'_F = \psi' \circ N_{F/Z}$ and $\psi_F = \psi \circ N_{F/Z}$. We note $\mathrm{Im}\,\psi' = \mathcal{U}$. We introduce $\mathcal{W}$ and $\mathcal{W}_{\mathcal{F}}$ for ψ and ψ_F, respectively. Namely, $\mathcal{W}$ (*resp.* $\mathcal{W}_{\mathcal{F}}$) is an $\mathbf{Z}_p\mathfrak{g}$-lattice defined to be the image of $\mathbf{Z}_p \otimes E_{1,Z}$ (*resp.* $\mathbf{Z}_p \otimes E_{1,F}$) by ψ (*resp.* ψ_F).

Let F_∞ be the cyclotomic $\mathbf{Z}_p$-extension of F. Let L_{F_∞} (*resp.* L_F) be the maximal unramified abelian pro-p-extension (*resp.* p-extension) of F_∞ (*resp.* F), where every prime ideal dividing p is totally decomposed. Denote by $L^*_{F_\infty}$ the maximal abelian extension of F contained in L_{F_∞}. Let $\overline{E}_{1,F}$ is the closed subgroup of $\prod_{\mathfrak{p} \in S_F} F^{\times}_{\mathfrak{p}}$ generated by the diagonal image of $E_{1,F}$. Let $J'_{\mathfrak{p},p}$ the image of $\overline{E}_{1,F}$ into $J_{F,p}$. We have $Gal(L^*_{F_\infty}/L_F)$ is isomorphic to the quotient group

$$\prod_{\mathfrak{p} \in S_F} F^{\times}_{\mathfrak{p}}/(\overline{E}_{1,F} \prod_{\mathfrak{p} \in S_F} NF^{\times}_{\mathfrak{p},\infty})$$

by class field theory. This group is canonically isomorphic to $J_{F,p}/J'_{F,p}$. By applying ψ'_F, we have

$$(5) \qquad Gal(L^*_{F_\infty}/L_F) \cong \mathcal{U}/\mathcal{W}_F.$$

$Gal(L^*_{F_\infty}/L_F)$ is a finitely generated $\mathbf{Z}_p$-module of $\mathbf{Z}_p$-rank one, because the Leopoldt conjecture and the Gross conjecture are valid for F, *c.f.* [5, Theorem 1]. Thus, $\mathcal{U}/\mathcal{W}_F$ is also finitely generated and of $\mathbf{Z}_p$-rank one. We note $e^-\mathcal{W}_F$ and e^-W_F have the same $\mathbf{Z}_p$-rank as $e^-\mathbf{Z}_p\mathfrak{g}$, because $e^-(\mathcal{U}/\mathcal{W}_F)$ and $e^-(U_F/W_F)$ are of finite order.

Lemma 2. *The restriction map of ψ_F (resp. φ_F) onto $\mathbf{Z}_p \otimes E^{2e^-}_{1,F}$ is an isomorphism onto $e^-\mathcal{W}_F$ (resp. e^-W_F). Hence, $e^-W_F \cong e^-\mathcal{W}_F$.*

Proof. Let $E_{0,F}$ be the group of units of F. Since p is odd and F does not contain any primitive pth root of unity, we have $\mathbf{Z}_p \otimes E^{2e^-}_{0,F} = 0$. Thus, $\mathbf{Z}_p \otimes E^{2e^-}_{1,F}$ maps onto e^-W_F, isomorphically. Furthermore, since restriction of ψ_F onto $\mathbf{Z}_p \otimes E^{2e^-}_{1,F}$ is surjection onto $e^-\mathcal{W}_F$ and since the rank of $e^-\mathcal{W}_F$ and e^-W_F are equal, we have $e^-W_F \cong e^-\mathcal{W}_F$. *q.e.d*

3 Lattices generated by Gauss sums. Let $\mathfrak{F}$ be a set of positive integers m such that $m \not\equiv 2 \mod 4$ and $p \nmid m$. We shall define a slightly modified Gauss sum for each pair $(\mathfrak{p}', m) \in S_F \times \mathfrak{F}$. Denote by $\mathfrak{P}$ an arbitrary extension onto $\mathbf{Q}(\zeta_m)$ of the prime ideal of $Z \cap \mathbf{Q}(\zeta_m)$ obtained by restricting $\mathfrak{p}'$. We denote by Z_m the decomposition field of p in $\mathbf{Q}(\zeta_m)$. We see $Z \cap \mathbf{Q}(\zeta_m) = Z \cap Z_m$. This subfield $Z \cap Z_m$ of Z_m is written as Z'_m in short. Let $\left(\frac{x}{\mathfrak{P}}\right)_m$ be the mth power residue symbol defined on $\mathbf{Q}(\zeta_m)$. A multiplicative character $\omega_{m,\mathfrak{P}}$ of the residue field of $\mathfrak{P}$ is defined by $\omega_{m,\mathfrak{P}}(x \mod \mathfrak{P}) = \left(\frac{x}{\mathfrak{P}}\right)_m$. Let ψ_p be an isomorphism of the additive group of the prime field $\boldsymbol{F}_p$ onto the group of pth roots of unity. Let $Tr_{\mathfrak{P}|p}$ be the trace map of the residue field $F_{\mathfrak{P}}$ onto $\boldsymbol{F}_p$. The Gauss sum $\mathcal{G}(\mathfrak{P})$ is an element of $\mathbf{Q}(\zeta_{mp})$ defined to be

$$\mathcal{G}(\mathfrak{P}) = \sum_{a \in F^{\times}_{\mathfrak{P}}} \omega_{m,\mathfrak{P}}(a)^{-1} \psi_p \circ Tr_{\mathfrak{P}|p}(a).$$

Denote by σ_c the image into the Galois group of $\mathbf{Q}(\zeta_{mp})$ of an integer c such that $(c, mp) = 1$ by the Artin map. Namely, σ_c is an element of the Galois group which maps ζ_{mp} to

ζ_{mp}^c. If $c \equiv 1 \mod m$, σ_c belongs to the subgroup $Gal(\mathbf{Q}(\zeta_{mp})/\mathbf{Q}(\zeta_m))$ and $\sigma_c\mathcal{G}(\mathfrak{P}) = \omega_{m,\mathfrak{P}}(c)\mathcal{G}(\mathfrak{P})$. Since $\sigma_c^{p-1} = 1$, we see $\omega_{m,\mathfrak{P}}(c)^{p-1} = 1$. Namely, $\mathcal{G}(\mathfrak{P})^{e_p} \in \mathbf{Q}(\zeta_m)$ for $e_p = p-1$. Moreover, $\mathcal{G}(\mathfrak{P})^{e_p}$ is fixed by the Frobenius automorphism at p of $\mathbf{Q}(\zeta_m)$, *c.f.* [6, the formula GS4 and GS5, §1, Chap. 1]. Therefore, it is an element of the decomposition field Z_m of $\mathfrak{P}$ in $\mathbf{Q}(\zeta_m)$. The Gauss sum $G_{\mathfrak{p}',m}$ corresponding to a pair $(\mathfrak{p}', m)$ is an element of Z'_m defined to be

$$G_{\mathfrak{p}',m} = N_{Z_m/Z'_m}\mathcal{G}(\mathfrak{P})^{e_p}.$$

Since $\sigma\mathcal{G}(\mathfrak{P}) = \mathcal{G}(\sigma\mathfrak{P})$ holds for an arbitrary element $\sigma \in Gal(\mathbf{Q}(\zeta_{mp})/\mathbf{Q}(\zeta_p))$, we have $\sigma G_{\mathfrak{p}',m} = G_{\sigma\mathfrak{p}',m}$. Let $\mathfrak{p}$ be restriction of $\mathfrak{p}'$ onto Z. It is obvious that $G_{\mathfrak{p}',m} = G_{\mathfrak{p},m}$ holds for the Gauss sum of Z defined for $(\mathfrak{p}, m) \in S \times \mathfrak{F}$. Let $E_{2,F}$ be a subgroup of the group of p-units of F generated by every $G_{\mathfrak{p}',m}$ when $(\mathfrak{p}', m)$ runs through every element of $S_F \times \mathfrak{F}$. We see $E_{2,F} = E_{2,Z}$. Let V (*resp.* $\mathcal{V}$) be the image of $\mathbf{Z}_p \otimes E_{2,Z}$ by φ (*resp.* ψ). V_F (*resp.* $\mathcal{V}_F$) denotes the image by φ_F (*resp.* ψ_F). We have $V_F = n_{F/Z}V$, $\mathcal{V}_F = n_{F/Z}\mathcal{V}$.

Let G_m be the Galois group of $\mathbf{Q}(\zeta_m)$. Let σ_a be the image of an integer a such that $(a, m) = 1$ by the Artin map onto G_m. The Stickelberger element θ_m is an element of the group ring $\mathbf{Q}G_m$ defined to be

$$\theta_m = \sum_{\substack{1\le a<m \\ (a,m)=1}} \tfrac{a}{m}\sigma_a^{-1}.$$

Let $\mathfrak{g}_m$ be the Galois group of Z_m. We denote by $\bar{\theta}_m$ the image of θ_m by the canonical homomorphism of $\mathbf{Q}G_m$ onto $\mathbf{Q}\mathfrak{g}_m$. Since $m\theta_m\mathfrak{P} = (\mathcal{G}(\mathfrak{P})^m)$ by the Stickelberger theorem and since $e_p\bar{\theta}_m \in \mathbf{Z}\mathfrak{g}_m$, *c.f.* [9, Lemma 6.14], we have $e_pm\bar{\theta}_m\mathfrak{P}_{|Z_m} = (\mathcal{G}(\mathfrak{P})^{e_pm})$. Therefore, the factorization of the principal ideal $(\mathcal{G}(\mathfrak{P})^{e_p})$ in Z_m is

$$(\mathcal{G}(\mathfrak{P})^{e_p}) = e_p\bar{\theta}_m \cdot \mathfrak{P}_{|Z_m}.$$

Put $\mathfrak{g}'_m = Gal(Z'_m/\mathbf{Q})$. Denote by $\bar{\theta}'_m$ the image of $\bar{\theta}_m$ by canonical restriction onto the group ring $\mathbf{Q}\mathfrak{g}'_m$. Let $\mathfrak{p}_m$ be restriction of $\mathfrak{p}$ onto Z'_m. By taking norm to Z'_m, we obtain the factorization of the principal ideal $(G_{\mathfrak{p}',m}) = (G_{\mathfrak{p},m})$ in Z'_m:

$$(G_{\mathfrak{p},m}) = e_p\bar{\theta}'_m \cdot \mathfrak{p}_m, \tag{6}$$

Note this gives $\varphi_Z(G_{\mathfrak{p},m})$ if we replace the prime ideal $\mathfrak{p}_m$ by the product of the prime ideals of Z dividing it.

Let n be a divisor of m contained in $\mathfrak{F}$. There is $\xi_{m,n} \in \mathbf{Z}\mathfrak{g}_n$ such that the image of $2e^-\theta_m$ onto $\mathbf{Q}\mathfrak{g}_n$ by the canonical map is $2e^-\xi_{m,n}\theta_n$. Precisely, $\xi_{m,n}$ is an element defined to be

$$\xi_{m,n} = \prod_{\substack{q|m \\ q\nmid n}} (1 - \sigma_q^{-1}),$$

where q denotes a prime number and σ_q denotes the Frobenius automorphism at q. Put $\eta_m = 2e^-e_p\bar{\theta}_m$. Since $\mathfrak{g}_m$ is commutative and since $N_{Z_m/Z'_n} = N_{Z_n/Z'_n} \circ N_{Z_m/Z_n}$, we have $N_{Z_m/Z'_n}(\eta_m\mathfrak{P}_{|Z_m})$ is equal to

$$N_{Z_n/Z'_n}(\eta_m N_{Z_m/Z_n}\mathfrak{P}_{|Z_m}).$$

Furthermore, we have $\eta_m N_{Z_m/Z_n}\mathfrak{P}_{|Z_m}$ equals $\xi_{m,n}\eta_n N_{Z_m/Z_n}\mathfrak{P}_{|Z_m}$. Therefore,

$$N_{Z_m/Z'_n}(\eta_m\mathfrak{P}_{|Z_m}) = \xi_{m,n}\eta_n\mathfrak{p}_n.$$

Since $\varphi_{Z|e^-\mathbf{Z}_p\otimes E_{2,Z}}$ is injective, the factorization (6) implies

$$N_{Z'_m/Z'_n}\left(1 \otimes G_{\mathfrak{p},m}^{2e^-}\right) = \xi_{m,n}\left(1 \otimes G_{\mathfrak{p},n}^{2e^-}\right) \tag{7}$$

holds.

Lemma 3. *e^-V is a $\mathbf{Z}_p\mathfrak{g}$-sublattice of e^-W of finite index.*

Proof. We may suppose $e^-W \neq 0$. Let $\hat{\mathfrak{g}}(-1)$ be a subset of the set of characters of $\mathfrak{g}$ satisfying $\chi(\rho) = -1$. We assume every character have their values in $\mathcal{K}$. Since $\mathcal{K}e^-W \cong e^-\mathcal{K}\mathfrak{g}$ follows from (4), the sublattice e^-V is of finite index if and only if $e_\chi\mathcal{K}\otimes V \neq 0$ for every character belonging to $\hat{\mathfrak{g}}(-1)$. Let ρ_χ be the $\mathcal{K}$-representation of the group ring $\mathcal{K}\mathfrak{g}$ affording the character χ. Let m be the conductor of χ as a primitive Dirichlet character. We have $\rho_\chi(\theta_m) = -L(0,\chi^{-1})$ from [9, Theorem 4.2]. Since χ is a character of the abelian field Z'_m, m is also the conductor of Z'_m. We see $\rho_\chi(\theta_m) = \rho_\chi(\bar{\theta}'_m)$ and $e_\chi\mathfrak{p}_m = (Z : Z'_m)e_\chi\mathfrak{p}$. Abbreviate the degree $(Z : Z'_m)$ to n_m. By (6), we obtain

(8) $\quad e_\chi\varphi_Z(1\otimes G^{2e^-}_{\mathfrak{p},m}) = 2e_pL(0,\chi^{-1})n_me_\chi\mathfrak{p}.$

$L(0,\chi^{-1}) \neq 0$ implies $e_\chi(1\otimes G^{2e^-}_{\mathfrak{p},m}) \neq 0$. *q.e.d*

Let e be an arbitrary idempotent element contained in $e^-\mathbf{Z}_pG$. Put

$$\begin{aligned} \ell_F &= \ell(eGal(\tilde{L}_F/F)), \\ \ell_F^* &= \ell(eGal(L^*_{F_\infty}/F)), \\ \ell_F^{**} &= \ell(eGal(L^*_{F_\infty}/F_\infty L^*_{Z_\infty})), \\ a_F &= \ell(eU_F/eV_F) - \ell(e\mathcal{U}/e\mathcal{V}_F), \\ b_F &= \ell_F - \ell_F^*, \\ c_F &= \ell(e\mathcal{V}/n_{F/Z}e\mathcal{V}). \end{aligned}$$

We have $e^-V_F \cong e^-\mathcal{V}_F$ from Lemma 2. Therefore, by Lemma 3, c_F is equal to the product of the $\mathbf{Z}_p$-rank of $e\mathbf{Z}_p\mathfrak{g}$ and $v_p(n_{F/Z})$.

Proposition 4. *We have $\ell_Z = a_Z + \ell_Z^*$. Moreover, $\ell_F = \ell_Z + \ell_F^{**} - c_F$.*

Proof. Since $e^-W_F/e^-V_F \cong e^-\mathcal{W}_F/e^-\mathcal{V}_F$, we have

$$a_F = \ell(eU_F/eW_F) - \ell(e\mathcal{U}/e\mathcal{W}_F).$$

Similarly,

$$b_F = \ell(eGal(\tilde{L}_F/L_F)) - \ell(eGal(L^*_{F_\infty}/L_F)).$$

$a_F = b_F$ follows from (4) and (5). In particular, since $eGal(\tilde{L}^*_{Z_\infty}/Z) = eGal(\tilde{L}^*_{Z_\infty}/Z_\infty)$,

$$\ell_Z = a_Z + \ell_Z^*.$$

We note $eU_F = n_{F/Z}eU$, $eV_F = n_{F/Z}eV$ and $e\mathcal{V}_F = n_{F/Z}e\mathcal{V}$. Thus, $a_Z - a_F = c_F$. We have

$$\ell_F = a_F + \ell_F^* = (\ell_Z - \ell_Z^*) + \ell_F^* - c_F.$$

In this equality, we substitute

$$\ell(eGal(F_\infty L^*_{Z_\infty}/F_\infty)) + \ell_F^{**}$$

for ℓ_F^*. Since $L^*_{Z_\infty} \cap F_\infty = Z_\infty$, we have $\ell(eGal(F_\infty L^*_{Z_\infty}/F_\infty))$ equals ℓ_Z^*. *q.e.d.*

Lemma 5. *We have the value of a_Z equals*

$$\sum_{\chi\in\Phi_e\cap\hat{\mathfrak{g}}} \ell(U_\chi/V_\chi) - \sum_{\chi\in\Phi_e\cap\hat{\mathfrak{g}}} \ell(\mathcal{U}_\chi/\mathcal{V}_\chi).$$

Proof. As $\mathbf{Z}_p\mathfrak{g}$-lattices, $eU \cong e\mathcal{U}$ and $eV \cong e\mathcal{V}$. Thus, in the equalities obtained by applying the formula (3) to eU/eV and to $e\mathcal{U}/e\mathcal{V}$, respectively, we have $\Delta(eU;eV) = \Delta(e\mathcal{U};e\mathcal{V})$. Hence, the difference $\ell(eU/eV) - \ell(e\mathcal{U}/e\mathcal{V})$ is equal to $\sum_{\chi\in\Phi_e}\ell(U_\chi/V_\chi) - \sum_{\chi\in\Phi_e}\ell(\mathcal{U}_\chi/\mathcal{V}_\chi)$. Moreover, if $\chi\notin\Phi_e\cap\hat{\mathfrak{g}}$, we have $e_\chi\mathcal{K}\otimes eU$ and $e_\chi\mathcal{K}\otimes e\mathcal{U}$ vanish. Hence, $U_\chi = \mathcal{U}_\chi = 0$. *q.e.d.*

Remark. Let H be the Galois group of F/Z. Let I_H be the ideal of $\mathbf{Z}_pG$ generated by $\{\sigma - 1 : \sigma \in H\}$. The canonical image of a primitive idempotent element $e \in \mathbf{Z}_pG$ into $\mathbf{Z}_p\mathfrak{g}$ is the trivial idempotent 0 if and only if $e \in I_H$. Hence, if $e^- \in I_H$, $e^-\mathbf{Z}_p\mathfrak{g}$ vanishes.

4. Proof of the formula (1).

Let $\tilde{L}_{F_\infty}$ be the maximal unramified abelian pro-

p-extension of F_∞. By [9, Corollary 13.29], $X_F = Gal(\tilde{L}_{F_\infty}/F_\infty)^{2e^-}$ is a $\mathbf{Z}_pG$-lattice. We shall prove in Lemma 6 in the below that $Y_F = e^-Gal(L_{F_\infty}/F_\infty)$ is also a $\mathbf{Z}_pG$-lattice. Let γ be a topological generator of $Gal(F_\infty(\zeta_p)/F(\zeta_p))$ satisfying $\zeta_{p^n}^\gamma = \zeta_{p^n}^{p+1}$ for every non-negative integer n. We restrict γ onto F_∞ and obtain a generator of $\Gamma = Gal(F_\infty/F)$. The action of T is defined by setting $T = \gamma - 1$ on an arbitrary $\mathbf{Z}_p[[\Gamma]]$-module. This makes X_F and Y_F $\mathbf{Z}_p[[T]]$-modules. Let $\hat{G}(-1)$ be the subset of $\hat{G} = \mathrm{Hom}(G, C_p^\times)$ consisting of characters taking a value -1 at the complex conjugation ρ.

Lemma 6. *Denote by A_F the Z_pG-module $Gal(\tilde{L}_{F_\infty}/L_{F_\infty})^{2e^-}$. Then, we have*

(1) *A_F is a $\mathbf{Z}_pG$-lattice which is isomorphic to $e^-\mathbf{Z}_p\mathfrak{g}$,*

(2) *Y_F is a $\mathbf{Z}_pG$-lattice which is isomorphic to X_F/A_F.*

Proof. Let S_n be the set of prime ideals dividing p in the nth layer F_n of the cyclotomic $\mathbf{Z}_p$-extension F_∞. Let U_n be the free $\mathbf{Z}_p$-module on the set S_n: $U_n = \oplus_{\mathfrak{p}_n \in S_n} \mathbf{Z}_p\mathfrak{p}_n$. U_0 is identified with the submodule p^nU_n. Let $\tilde{L}_{F_n}$ be the maximal unramified abelian p-extension of F_n. Let L_{F_n} be the maximal subfield where every prime ideal contained in S_n is decomposed totally. Let E_{1,F_n} be the group of p-units of F_n. Each element x of E_{1,F_n} is mapped into U_n by $\sum_{\mathfrak{p}_n \in S_n} p^n v_p(\iota_{\mathfrak{p}_n}(x))\mathfrak{p}_n$, where $\iota_{\mathfrak{p}_n}$ is an embedding of F_n into $\mathbf{C}_p$ corresponding to $\mathfrak{p}_n$. This map is extended onto $\mathbf{Z}_p \otimes E_{1,F_n}$. Let W_n be the image of $\mathbf{Z}_p \otimes E_{1,F_n}$ into U_n. We have $U_n/W_n \cong Gal(\tilde{L}_{F_n}/L_{F_n})$. Thus, $\varprojlim U_n/W_n \cong Gal(\tilde{L}_{F_\infty}/L_{F_\infty})$. We have $\mathbf{Z}_p \otimes E_{1,F_n}^{2e^-} \cong e^-W_n$, because $\mathbf{Z}_p \otimes E_{0,F_n}^{2e^-} = 0$ holds for the unit group E_{0,F_n} of F_n. This isomorphism induces an isomorphism between cohomology groups:

$$H^0(Gal(F_n/F), \mathbf{Z}_p \otimes E_{1,F_n}^{2e^-})$$
$$= \mathbf{Z}_p \otimes E_{1,F}^{2e^-}/\mathbf{Z}_p \otimes N_{F_n/F}(E_{1,F_n}^{2e^-})$$

and

$$H^0(Gal(F_n/F), e^-W_n) = e^-W_n/p^ne^-W_n.$$

Since the image of $\mathbf{Z}_p \otimes E_{1,F}^{2e^-}$ into e^-W_n coincides with e^-W_0, we have $e^-W_0 + p^ne^-W_n = e^-W_n$. This implies $e^-W_0 = e^-W_n$. Therefore, there is a sequence of surjective homomorphisms:

$$e^-U_n \to e^-U_n/e^-W_n \to e^-U_n/p^ne^-U_n.$$

We take the inverse limits for these three terms with respect to norm maps, respectively. We see both modules $\varprojlim e^-U_n$ and $\varprojlim e^-U_n/p^ne^-U_n$ are isomorphic to $e^-\mathbf{Z}_p\mathfrak{g}$. Therefore, $A_F \cong \varprojlim e^-U_n/e^-W_n \cong e^-\mathbf{Z}_p\mathfrak{g}$.

We see $Y_F \cong X_F/A_F$. Let C_n be the p-Sylow subgroup of the quotient group of the ideal class group of F_n by a subgroup generated by every prime ideal contained in S_n. We have $C_n \cong Gal(L_{F_n}/F_n)$. Denote by $i_{n,m}$ for $n > m$ the natural map of C_m into C_n. Let C be the inverse limit of C_n with respect to norm maps. Since $Y_F \cong e^-C$, Y_F is a Z_p-lattice if and only if e^-C dose. Let T_C be the maximal torsion subgroup of e^-C. By the same argument as the proof in [9, Proposition 13.28], it is proved that the multiplication p is injective on T_C if $i_{n+1,n}$ is injective on e^-C_n for every n. Namely, by [4, Theorem 12], we have Ker $i_{n+1,n}$ is isomorphic to the cohomology group $H^1(Gal(F_{n+1}/F_n), E_{1,F_{n+1}})$. Since F_{n+1} is an abelian extension and since this cohomology group is p-primary torsion, we have $e^- H^1(Gal(F_{n+1}/F_n), E_{1,F_{n+1}}) \cong H^1(Gal(F_{n+1}/F_n), \mathbf{Z}_p \otimes E^{2e^-}_{1,F_{n+1}})$. Moreover, the last cohomology group is isomorphic to $H^1(Gal(F_{n+1}/F_n), e^- W_{n+1})$. Here, $e^- W_{n+1}$ is a $\boldsymbol{Z}_p$-lattice where the Galois group of F_{n+1}/F_n acts trivially. Thus, the cohomology group vanishes. Hence, the multiplication by p is injective on $e^- C$. It follows $e^- C$ is p-torsion free. *q.e.d.*

We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & A_F & \to & X_F & \to & Y_F & \to 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \to & A_Z & \to & X_Z & \to & Y_Z & \to 0, \end{array}$$

where the vertical arrows are restriction maps of elements of Galois groups. In this diagram, the homomorphism of Y_F into Y_Z is surjective, because $L_{Z_\infty} \cap F_\infty = Z_\infty$. We recall $\mathcal{O}$ is a valuation ring of a finite extension of $\mathbf{Q}_p$ containing the set $\chi(G)$ for every $\chi \in \hat{G}$ and Λ is the ring of power series with coefficient in $\mathcal{O}$. We consider $\Lambda = \mathcal{O} \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[T]]$ to define its action on $X_{F,\chi}$, $Y_{F,\chi}$ and $A_{F,\chi}$, etc. Let f_χ (*resp.* g_χ) be the characteristic polynomial of a Λ-module X_F^χ (*resp.* Y_F^χ) for each χ belonging to $\hat{G}(-1)$. We see this is the characteristic polynomial of $X_{F,\chi}$ (*resp.* $Y_{F,\chi}$). Moreover, we see from the upper exact sequence in the above diagram that the characteristic polynomial f_χ of $X_{F,\chi}$ is divisible by that of $Y_{F,\chi}$. If $\chi \in \hat{\mathfrak{g}}$, we have $A_{\chi,F} \cong \mathcal{O}$ by Lemma 6. Thus, f_χ equals Tg_χ.

To obtain more detailed relation between the modules $X_{F,\chi}$, $Y_{F,\chi}$ and $Y_{Z,\chi}$, we need the main theorem of Iwasawa theory. Let h_χ be the power series in $\Lambda = \mathcal{O}[[T]]$ such that

$$L_p(s, \chi^{-1}\omega) = h_\chi((1+p)^s - 1)$$

holds, where ω is the Teichmüller character and $L_p(s, \chi^{-1}\omega)$ is the p-adic L-function relative to the character $\chi^{-1}\omega$. By the main theorem of Iwasawa theory, h_χ associates to the characteristic polynomial f_χ. Namely, there is a unit power series u_χ satisfying

$$h_\chi = f_\chi u_\chi \tag{9}$$

c.f. [7, Chap. 1, §6] and [9, §13.6]. By setting $s = 0$ in $T = (1+p)^s - 1$ in these formula, we have

$$v_p(f_\chi(0)) = v_p(L_p(0, \chi^{-1}\omega)). \tag{10}$$

The value of $v_p(L_p(0, \chi^{-1}\omega))$ equals

$$v_p(L(0, \chi^{-1})) + v_p(1 - \chi^{-1}(p)). \tag{11}$$

We note $\chi(p) = 1$ if and only if $\chi \in \hat{\mathfrak{g}}$. Suppose $\chi \in \hat{\mathfrak{g}} \cap \hat{G}(-1)$. Let $\bar{f}_\chi$ be the characteristic polynomial of $X_{Z,\chi}$. We also have $\bar{f}_\chi$ associates to h_χ by applying the main theorem to Z. Hence, $f_\chi = \bar{f}_\chi$. It follows from the lower sequence in the above diagram that $g_\chi = f_\chi T^{-1}$ is also the characteristic polynomial of $Y_{Z,\chi}$. In consequence, $Y_{F,\chi}$ and $Y_{Z,\chi}$ are free $\mathcal{O}$-modules of the same rank. Since the surjection of Y_F onto Y_Z induces a surjective $\mathcal{O}$-homomorphism of $Y_{F,\chi}$ onto $Y_{Z,\chi}$, we have $Y_{F,\chi} \cong Y_{Z,\chi}$. If $\chi \notin \hat{g}$, we have $A_{F,\chi} = 0$ from Lemma 6. Hence, $f_\chi = g_\chi$. Furthermore, we have $X_{F,\chi} \cong Y^*_{F,\chi}$, and obtain $X_{F,\chi} \cong Y_{F,\chi}$, because $X_{F,\chi}$ is $\mathcal{O}$-torsion free.

Lemma 7. *Set* $\Phi'_e = \Phi_e \backslash \hat{\mathfrak{g}}$. *We have* $\ell_F^{**} = \sum_{\chi \in \Phi'_e} v_p(L(0, \chi^{-1})) + c_F$.

Proof. Since $e^{-}Gal(L^*_{F_\infty}/F_\infty)$ (*resp.* $e^{-}Gal(L^*_{Z_\infty}/Z_\infty)$) equals Y_F/TY_F (*resp.* Y_Z/TY_Z), we have an exact sequence

$$0 \to e^{-}Gal(L^*_{F_\infty}/L^*_{Z_\infty}F_\infty) \to Y_F/TY_F \to Y_Z/TY_Z \to 0.$$

Therefore, $\ell^{**}_F = \ell(eY_F/TeY_F) - \ell(eY_Z/TeY_Z)$. We shall apply Lemma 1 to these two terms. If $\chi \in \Phi_e \cap \hat{\mathfrak{g}}$, we have $Y_{F,\chi} \cong Y_{Z,\chi}$. Hence, $\ell(Y_{F,\chi}/TY_{F,\chi}) = \ell(Y_{Z,\chi}/TY_{Z,\chi})$. If $\chi \in \Phi'_e$, we have $Y_{Z,\chi} = 0$ and $X_{F,\chi} \cong Y_{F,\chi}$. Consequently,

$$\ell^{**}_F = \sum_{\chi\in\Phi'_e} \ell(X_{F,\chi}/TX_{F,\chi}).$$

By Lemma 1, this value of the sum is equal to $\sum_{\chi\in\Phi'_e} v_p(f_\chi(0))$. Let $\hat{\mathfrak{g}}_p$ be the group of characters of the p-Sylow subgroup of $\mathfrak{g}$. Since a character $\chi \in \hat{G}(-1)$ is a product of $\chi_0 = \chi_{|G_0}$ and $\chi_p = \chi_{|G_p}$, it does not belong to $\hat{\mathfrak{g}}$ if and only if the condition (i) $\chi_0 \notin \hat{\mathfrak{g}}$ or (ii) $\chi_0 \in \hat{\mathfrak{g}}$ and $\chi_p \notin \hat{\mathfrak{g}}_p$ is satisfied. Since the Frobenius automorphism on p generates $Gal(F/Z)$, we see $v_p(1-\chi^{-1}(p)) = 0$ if the condition (i) holds. Let H_p be the p-Sylow subgroup of the cyclic group $Gal(F/Z)$. We have an exact sequence of the groups of characters: $1 \to \hat{\mathfrak{g}}_p \to \hat{G}_p \to \hat{H}_p \to 1$. Let ψ be a character of $\hat{G}_p$ whose restriction onto H_p generates $\hat{H}_p$. Assume H_p is of order p^d. Note p^d is the maximal power of p dividing $n_{F/Z}$. We see $\hat{G}_p\backslash\hat{\mathfrak{g}}_p = \{\chi\psi^i : \chi \in \hat{\mathfrak{g}}_p, 1 \le i < p^d\}$. Let Φ''_e be the subset of Φ'_e comprising characters satisfying (ii). Since $\Phi''_e = \{\chi\psi^i : \chi \in \hat{\mathfrak{g}}, \rho_\chi(e) \neq 0, 1 \le i < p^d\}$, $\sum_{\chi\in\Phi'_e} v_p(f_\chi(0))$ is equal to

$$\sum_{\chi\in\Phi'_e} v_p(L(0,\chi^{-1})) + \sum_{\chi\in\Phi''_e} v_p(1-\chi^{-1}(p))$$

from (10) and (11). Here, the sum concerning Φ''_e in the right is equal to

$$\sum_{\chi\in\hat{\mathfrak{g}}\cap\Phi_e} \sum_{i=1}^{p^d-1} v_p(1-\psi^i(p)^{-1}).$$

Let ϕ be the Euler function. Note $\psi(p)$ is a primitive p^dth root of unity. Since the number of primitive p^{d-i}th roots of unity equals $\phi(p^{d-i})$, the value of this sum is equal to

$$\sum_{\chi\in\hat{\mathfrak{g}}\cap\Phi_e} \sum_{i=0}^{d-1} v_p(1-\zeta_{p^d}^{-p^i})\phi(p^{d-i}).$$

Hence, it is equal to $d\sharp(\hat{\mathfrak{g}}\cap\Phi_e)$. Since $\sharp(\hat{\mathfrak{g}}\cap\Phi_e) = \mathrm{rank}_{\mathbf{Z}_p} e\mathbf{Z}_p\mathfrak{g} = \mathrm{rank}_{\mathbf{Z}_p} e\mathcal{V}$, we have $\ell^{**}_F = \sum_{\chi\in\Phi'_e} v_p(L(0,\chi^{-1})) + c_F$. *q.e.d.*

Lemma 8. *Let m be the conductor of $\chi \in \hat{\mathfrak{g}} \cap G(-1)$ and let $\mathfrak{p}$ be a prime ideal of Z dividing p. $e_p = p-1$ and $n_m = [Z : Z'_m]$, where $Z'_m = Z \cap Z_m$. Then, we have*
(i) $e_\chi\varphi_Z(G_{\mathfrak{p},m}) = e_p n_m L(0,\chi^{-1})(e_\chi\mathfrak{p})$,
(ii) $e_\chi\psi_Z(G_{\mathfrak{p},m}) = (e_p n_m/p)L'_p(0,\chi^{-1}\omega)(e_\chi\iota_{\mathfrak{p}})$.

Proof. Since $\chi \in \hat{\mathfrak{g}}$, it is a character of the abelian field Z'_m. Thus, the conductor of Z'_m is equal to m. We have (i) from (8). Let $\iota_{\mathfrak{p}_m}$ be restriction of $\iota_{\mathfrak{p}}$ onto Z'_m. By the right action $G^\sigma_{\mathfrak{p},m}$ of σ, we mean it acts as $\sigma^{-1}G_{\mathfrak{p},m}$ from the left. We see $e_\chi\psi_Z(G_{\mathfrak{p},m}) = \frac{1}{p}e_\chi\sum_{\sigma\in\mathfrak{g}}\log_p\left(\iota_{\mathfrak{p}}(G^\sigma_{\mathfrak{p},m})\right)\iota_{\sigma\mathfrak{p}}$. Put $A = e_\chi\psi_Z(G_{\mathfrak{p},m})$. We have

$$A = \frac{1}{p}\sum_{\sigma\in\mathfrak{g}} \chi(\sigma)\log_p(\iota_{\mathfrak{p}}(G^\sigma_{\mathfrak{p},m}))(e_\chi\iota_{\mathfrak{p}}).$$

Let $\mathfrak{g}'_m$ (*resp.* $\mathfrak{h}_m$) be the Galois group of $Z'_m/\mathbf{Q}$ (*resp.* Z/Z'_m). Since $G_{\mathfrak{p},m} \in Z'_m$, A is equal to

$$\frac{1}{p}\sum_{\sigma'\in\mathfrak{g}'_m} \chi(\sigma')\sum_{h\in\mathfrak{h}_m} \log_p(\iota_{\mathfrak{p}_m}(G^{\sigma'}_{\mathfrak{p},m}))(e_\chi\iota_{\mathfrak{p}}).$$

Furthermore, since $|\mathfrak{h}_m| = n_m$, this equals

$$(12)\quad \frac{n_m}{p}\sum_{\sigma'\in\mathfrak{g}'_m} \chi(\sigma')\log_p(\iota_{\mathfrak{p}_m}(G^{\sigma'}_{\mathfrak{p},m}))(e_\chi\iota_{\mathfrak{p}}).$$

Let $\mathfrak{P}$ be an arbitrary prime ideal of $\mathbf{Q}(\zeta_m)$ dividing $\mathfrak{p}_m$. Put $\mathfrak{h}'_m = Gal(Z_m/Z'_m)$. Let $\{\sigma_1, \cdots, \sigma_d\}$ be a set of representatives of $\mathfrak{g}'_m$ in $\mathfrak{g}_m = Gal(Z_m/\mathbf{Q})$. Let $\{\sigma_{i1}, \cdots, \sigma_{if}\}$ be the coset $\sigma_i \mathfrak{h}'_m$. Denote by $\tilde{\sigma}_{ij}$ an arbitrary extension of σ_{ij} onto $\mathbf{Q}(\zeta_m)$. There is an integer c_{ij} for each σ_{ij} such that $\tilde{\sigma}_{ij}\zeta_m = \zeta_m^{c_{ij}}$ holds. This integer is determined up to the subgroup generated by p in $(\mathbf{Z}/m\mathbf{Z})^\times$. Since $\chi(p) = 1$, we have $\chi(c_{ij}) = \chi(\sigma_{ij}) = \chi(\sigma_i)$. By the definition (6) of our Gauss sums, we see $\chi(\sigma_i)\log_p(\iota_{\mathfrak{p}_m}(G_{\mathfrak{p},m}^{\sigma_i}))$ coincides with

$$\sum_{j=1}^{f} \chi(\sigma_i) \log_p(\iota_{\mathfrak{P}}(\mathcal{G}(\mathfrak{P})^{e_p\sigma_{ij}})),$$

where $\iota_{\mathfrak{P}}$ is an embedding of $\mathbf{Q}(\zeta_m)$ into C_p which is extension of $\iota_{\mathfrak{p}}$ onto $\mathbf{Q}(\zeta_m)$ and corresponding to $\mathfrak{P}$. Put $g_{ij} = \mathcal{G}(\mathfrak{P})^{e_p\sigma_{ij}}$. We observe

$$g_{ij} = \left(\sum_{a \in F_{\mathfrak{P}}^\times} \omega_{m,\mathfrak{P}}^{c_{ij}}(a) \psi_p \circ Tr_{\mathfrak{P}|p}(a) \right)^{e_p}.$$

Thus, the value of $\sum_{i=1}^{d} \chi(\sigma_i) \log_p(\iota_{\mathfrak{p}_m}(G_{\mathfrak{p},m}^{\sigma_i}))$ is equal to

$$\sum_{i,j} \chi(c_{ij}) \log_p \circ \iota_{\mathfrak{P}}(g_{ij}).$$

This value equals $e_p L'_p(0, \chi^{-1}\omega)$ from [6, Theorem 3.2, Chap.17]. We have the formula (ii) from (12).

Now, we can prove the main result:

Theorem 9. *Let F be a finite abelian extension where the prime p is unramified. Let e be an idempotent element contained in $e^- \mathbf{Z}_p G$. Then, the formula* (1) *is valid.*

Proof. We observe from Proposition 4 and Lemma 7 that the formula (1) holds for F if it is valid for Z. Since all of modules $e^- Gal(\tilde{L}_Z/Z)$, $e^- Gal(\tilde{L}_Z^*/Z_\infty)$, $e^- U$ and $e^- \mathcal{U}$ appearing the first formula in Proposition 4 are $\mathbf{Z}_p\mathfrak{g}$-modules, we may restrict the idempotent e onto $\mathbf{Z}_p\mathfrak{g}$. So, we study the case $F = Z$. e is a non-trivial idempotent contained in $e^- \mathbf{Z}_p\mathfrak{g}$. Let χ be a character belonging to Φ_e. Let m be the conductor of χ. Let K be the fixed field by a subgroup Ker χ of $\mathfrak{g}$. We notice $K = Z'_m$. Let $g_n = e_\chi(1 \otimes G_{\mathfrak{p},n})$ be the image of $1 \otimes G_{\mathfrak{p},n}$ into $(\mathbf{Z}_p \otimes E_{2,Z}^{2e^-})_\chi$ for $n \in \mathfrak{F}$. Write E_χ for $(\mathbf{Z}_p \otimes E_{2,Z}^{2e^-})_\chi$. Suppose $m \nmid n$ and put $d = (m, n)$. We see $d < m$. If $K \subset Z'_n$, K is a subfield of $Z'_m \cap Z'_n$. Since $Z'_m \cap Z'_n$ is a subfield of $\mathbf{Q}(\zeta_m) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_d)$, the conductor of K is a divisor of d. This is not the case. Thus, $K \not\subset Z'_n$. Put $\delta = \sum_{\sigma \in Gal(Z/K)} \sigma$. $x = G_{\mathfrak{p},n}$ is an element of Z'_n and $\delta x = N_{Z'_n/K \cap Z'_n}(x)^{[Z:Z'_n K]}$. Hence, $\delta x \in K \cap Z'_n$. This implies $e_\chi \delta g_n = 0$, because of $Z'_n \neq K \cap Z'_n$. On the other hand, since $e_\chi \delta = [Z : K] e_\chi$, we have $\delta g_n = [Z : K] e_\chi g_n$. Therefore, $g_n = 0$. Next, we suppose $m \mid n$. We have

$$(Z'_n : Z'_m) g_n = \chi(\xi_{n,m}) g_m$$

from (7). Hence, $g_n = 0$ if $\chi(\xi_{n,m}) = 0$. If $\chi(\xi_{n,m}) \neq 0$, then there are $a_n \in \mathcal{O}^\times$ and an integer c_n such that

$$g_n = a_n \pi^{c_n} g_m$$

holds for a prime element π of $\mathcal{O}$. Since E_χ is a finitely generated $\mathcal{O}$-module, there is the minimum in the integers c_n for $m \mid n$. Let c be the minimum value. We have $E_\chi = \mathcal{O}\pi^c g_m$. Hence, V_χ and $\mathcal{V}_\chi$ are generated by $\pi^c e_\chi \varphi(G_{\mathfrak{p},m})$ and $\pi^c e_\chi \psi(G_{\mathfrak{p},m})$, respectively.

Put $\varepsilon = v_p(n_m) + v_p(\pi^c)$. Since U_χ (*resp.* $\mathcal{U}_\chi$) is generated by $e_\chi \mathfrak{p}$ (*resp.* $e_\chi \iota_{\mathfrak{p}}$) over $\mathcal{O}$, we observe

$$\ell(U_\chi/V_\chi) = v_p(L(0,\chi^{-1})) + \varepsilon,$$

$$\ell(\mathcal{U}_\chi/\mathcal{V}_\chi) = v_p(L'_p(0,\chi^{-1}\omega)) - 1 + \varepsilon$$

from Lemma 8. Furthermore, $\ell^*_Z = v_p(g_\chi(0))$ from Lemma 1. Hence, by Proposition 4 and Lemma 5, ℓ_Z equals the value of

$$\sum_{\chi\in\Phi_e} v_p(L(0,\chi^{-1})) + \sum_{\chi\in\Phi_e} v_p(g_\chi(0)) - \sum_{\chi\in\Phi_e} \left(v_p(L'_p(0,\chi^{-1}\omega)) - 1\right).$$

Therefore, the formula (1) follows if we show an equality

$$v_p(g_\chi(0)) = v_p(L'_p(0,\chi^{-1}\omega)) - 1 \tag{13}$$

holds. This equation is a consequence of the main theorem of Iwasawa theory. Namely, put $a_p = p+1$ and $y = a_p^s - 1$. By (9), we have $L'_p(s,\chi^{-1}\omega)$ equals

$$(f'_\chi(y)u_\chi(y) + f_\chi(y)u'_\chi(y))a_p^s \log_p a_p.$$

Since $f_\chi = Tg_\chi$, we obtain

$$L'_p(0,\chi^{-1}\omega) = g_\chi(0)u_\chi(0)\log_p a_p$$

by setting $s=0$. This proves (13).

5 The structure of $e\mathbf{Z}_p \otimes C_F$. Let m be the order of G_p. Put $\hat{G}_0(-1) = \hat{G}_0 \cap \hat{G}(-1)$. The Galois group of $\mathbf{Q}_p(\zeta_m)/\mathbf{Q}_p$ acts on the sets $\hat{G}_0(-1)$ and $\hat{G}_p$. Let χ'_0 (*resp.* χ'_p) be a conjugate character of $\chi_0 \in \hat{G}_0(-1)$ (*resp.* $\chi_p \in \hat{G}_p$). We see

$$v_p(L(0,\chi_0\chi_p)) = v_p(L(0,\chi'_0\chi'_p)).$$

For a conjugacy class c_0 (*resp.* c_p) of $\hat{G}_0$ (*resp.* $\hat{G}_p$), we see c_0c_p is the conjugacy class containing the character $\chi = \chi_0\chi_p$. Note $\sharp c_p = \phi(|\chi_p|)$. Put

$$c_\chi = v_p(L(0,\chi)).$$

Let e be a primitive idempotent such that $\chi_0(e) \neq 0$. Let $\{c_{p,i}\}_{i=1}^s$ be the set of conjugacy classes of $\hat{G}_p$ and let $\chi_{p,i}$ be the representatives of the class $c_{p,i}$. We have

$$v_p(\sharp e\mathbf{Z}_p \otimes C_F) = \sum_{i=1}^{s} \sharp c_0 \sharp c_{p,i} \cdot c_{\chi_0\chi_{p,i}}$$

from the theorem. Let p^d be the order of χ_p. Let H be the kernel of χ_p. The fixed field of H is a compositum of F^{G_0} and a cyclic extension over $\mathbf{Q}$ of degree p^d. Let $(F^H)_0$ be the cyclic subextension of degree p^{d-1} over F^{G_0} contained in F^H. Since a prime is totally ramified in $F^H/(F^H)_0$, the norm map is surjection of C_{F^H} onto $C_{(F^H)_0}$. Denote by N_0 the norm map. Let e be a primitive idempotent element such that $\chi_0(e) \neq 0$. Put $C(e;c_p) = e\mathbf{Z}_p \otimes \operatorname{Ker} N_0$. We see the value of $v_p(\sharp C(e;c_p))$ equals

$$v_p(\sharp e\mathbf{Z}_p \otimes C_{F^H}) - v_p(\sharp e\mathbf{Z}_p \otimes C_{(F^H)_0}).$$

If we apply the theorem to these two terms, we obtain

$$v_p(\sharp C(e;c_p)) = \sharp c_0 \phi(|\chi_p|)c_\chi.$$

This formula was essentially proved in [8] when G_p is a cyclic group. If we consider the natural map

$$i_{c_p} : C(e;c_p) \to e\mathbf{Z}_p \otimes C_F$$

when c_p runs through every conjugacy class of $\hat{G}_p$, we have a homomorphism

$$i_e : \bigoplus_{c_p} C(e;c_p) \to e\mathbf{Z}_p \otimes C_F.$$

If this map is surjective, it is an isomorphism of $\mathbf{Z}_pG$-modules, because the order of these two modules is equal. However, if we take account of the formula of generators of $e\mathbf{Z}_p \otimes C_F$ as a $\mathbf{Z}_pG$-module given in [10], this is not always true.

Our second remark is that the proof of the theorem is essential in the case $F = Z$. Let e be an idempotent element of $e^-\mathbf{Z}_pG$ such that

$e\mathbf{Z}_p\mathfrak{g}$=0. We have $eA_F = 0$ and $eX_F \cong eY_F$. Hence, the order of $N = eX_F/TeX_F$ is finite. Let t be the canonical surjection of N onto $eGal(\tilde{L}_F/F)$. If t is an isomorphism, we have the formula (1) for e from Lemma 1 and the formulas (10) and (11). Moreover, we also have

$$\ell(N_\chi^*) = v_p(L(0,\chi^{-1}))$$

holds. We can prove by studying the genus group of F_∞/F that t is isomorphic.

References.

[1] C. W. Curtis, I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Orders I, John Willy & Sons, 1981.

[2] L. Federer, B. H. Gross, Regulator and Iwasawa modules, Invent. Math. 62(1981) 443–457.

[3] C. Greither, Class groups of abelian fields, and the main conjecture, Ann. Inst. Fourier, Grenoble 42 (1992) 449–499.

[4] K. Iwasawa, On Z_l-extension of algebraic number fields, Annals of Math. 98 (1973) 246–326.

[5] J.-F. Jaulent, Sur les conjecture de Leopoldt et de Gross, Soci. Math. de France Astérisque 147–148 (1987) 107–120.

[6] S. Lang, Cyclotomic Fields, Graduate Texts in Math., vol. 121, Springer, New York, 1990.

[7] B. Mazur and A. Wiles, Class group of abelian extensions of $\mathbf{Q}$, Invent. Math. 76 (1986) 179–330.

[8] D. Solomon, On the class group of imaginary abelian fields, Ann. Inst. Fourier, Grenoble **40**(1990), 467–492.

[9] L. C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Math., vol. 83, Springer, New York, 1996.

[10] H. Yamashita, On the rank of the first radical layer of a p-class group of an algebraic number field, Nagoya Math. J. 156(1999), 85–108.

[11] H. Yamashita, The relative p-class number formula of an abelian field, J. of Kanazawa Gakuin Univ. Information and Natural Sci. 3 (2005) 73-88.